NOKIA

Cloud DCI for government

Enabling data center consolidation and shared infrastructure for the government cloud

White paper

State and local governments, as well as public sector agencies are under pressure to modernize ICT to ensure sustainable, reliable, secure, anytime connectivity for citizens, businesses and employees. Cloud computing supported by a more dynamic communications network offers a more agile and flexible framework to meet future government ICT needs. Implementing a government cloud enables government departments and public sector agencies to share information and resources while achieving greater coherence and economies of scale, giving citizens and employees secure online access to applications, services and data in the cloud.

Cloud DCI—also called cloud interconnect—provides a more agile and dynamic approach to connect data centers in a secure private cloud of virtualized compute and storage. These virtualized data centers can use SDN to automatically allocate resources and balance workloads across multiple servers, sites and cloud types. Nokia offers a choice of cloud DCI solutions that provide the scalability, performance and security to support current DCI needs—long with the agility, flexibility and capacity required to interconnect data centers in private and hybrid clouds.

NOKIA

Contents

NOKIA

Introduction

State and local governments and government agencies, as well as the public sector, are under pressure to modernize information communications infrastructure (ICT). Government and public sector ICT is typically characterized by silos of infrastructure, high levels of duplication, service fragmentation and poor levels of resource utilization. Aging ICT infrastructure needs to be consolidated and transformed to ensure sustainable, reliable, secure, anytime access to data for citizens, businesses and employees.

Much of this data is sensitive government or personal data that has traditionally been stored and processed securely and reliably in government and public sector data centers. Typically, data center interconnect (DCI) using secure network infrastructure connects primary, backup, and remote data centers. Long-established data backup procedures provide business continuity and disaster recovery (BCDR) in the event of technical failures or major incidents.

New technologies, such as virtualized architecture and software-defined networking (SDN), greatly improve data center efficiency, simplify operations and increase agility. Consequently, governments and public sector agencies are very interested in understanding the value of these technologies.

In addition, cloud computing supported by a dynamic communications network promises a more agile and flexible framework to meet future government ICT needs. Implementing a government cloud enables government departments and public sector agencies to share information and resources while achieving greater coherence and economies of scale. Key to this is consolidating and virtualizing data centers in the cloud to improve efficiency and significantly reduce costs.

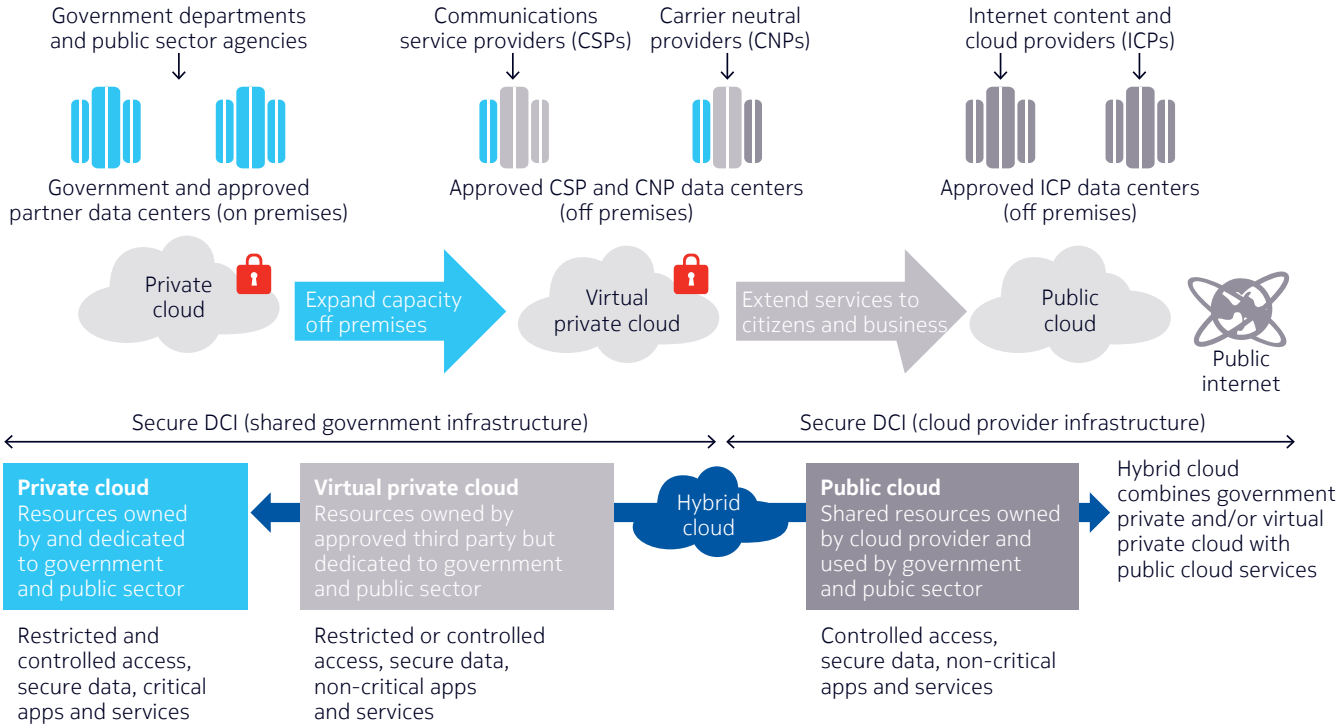
Cloud DCI allows government departments and public sector agencies to connect on-premises data centers in a secure private cloud of virtualized compute and storage. Cloud DCI can also be used to augment private cloud data centers with IT assets hosted in off-premises third-party data centers; for example, in government-approved service provider or carrier-neutral collocation facilities or to enable outsourcing of non-critical IT needs to public cloud providers.

This approach allows government departments and public sector agencies to implement a government cloud that that is more agile, flexible and cost effective. Using the right mix of private, virtual private and hybrid cloud models that embrace public cloud services enables governments and the public sector to better match cost models to their business requirements.

Cloud models for government and public sector

Figure 1 shows how government and the public sector might implement different types of cloud. These are described in this section and more fully in the Nokia white paper Cloud Interconnect for enterprise and public sector, which also outlines how to achieve the right cloud balance.

Figure 1. Types of cloud and how they might be used to implement government cloud



Government private cloud

A government private cloud typically consists of on-premises data centers and the DCI network that interconnects them securely over shared government infrastructure. This infrastructure is also often used to connect government and public sector offices in different locations.

A government private cloud is usually controlled by a single authority, and may be operated by the government itself or on its behalf by an approved partner. It typically runs critical applications and services that handle confidential data and information. Government private clouds have restricted access and the highest levels of authentication, control, data sovereignty and security.

Typically, a private DCI network using shared government infrastructure connects data centers in the same regional area to enable synchronization of data between data centers for BCDR. In many cases, data centers in another region provide additional resiliency in case of major incidents. Such private clouds—also known as on-premises clouds—can support virtualization to allow IT assets to be quickly assigned and shared; for example, to distribute workloads or reassign capacity for short-term projects.

Government virtual private cloud

Virtual private clouds allow governments and public sector agencies to expand their private clouds cost effectively. They can add data center resources owned by an approved third party, such as a communications service provider (CSP) or carrier-neutral provider (CNP), but dedicated to their use. The government private cloud connects securely to a CSP multi-tenant data center (MTDC) or CNP collocation facility by extending the government's private DCI network or by using an approved secure managed DCI service. Virtual private clouds have several benefits:

- Assets or resources become an extension of the government private cloud but are located off-premises in third-party data center facilities.
- Like virtual private networks (VPNs), these assets or resources are completely isolated and kept separate and secure from other organizations' assets and resources.
- The government can install and manage its own compute, storage and network assets and pay only for space and power, or they can lease resources from the provider.
- Different options are available from bare metal servers to dedicated infrastructure as a service (IaaS), platform as a service (PaaS) or software as a service (SaaS) solutions.

Virtual private clouds—also known as hosted clouds—provide greater flexibility for less critical business operations. They also allow CAPEX and OPEX to be matched to IT needs, without sacrificing performance, control and security. Typically, a virtual private cloud runs non-critical applications and services, hosts non-sensitive data securely and has restricted or controlled access. Virtual private clouds can be used to enable citizens and businesses to access government and public sector services in a controlled and secure way.

Government use of public cloud services

Public clouds provide another way to augment private clouds using resources or services provided by an internet cloud provider (ICP). Cloud resources and services are used on a pay-as-you-go basis and can be used dynamically to scale compute and storage or deliver services on demand. In other words, the government only pays for the resources and services it consumes, based on the time for which they are used. Public cloud resources and services remain completely separate from the government's private and virtual private cloud.

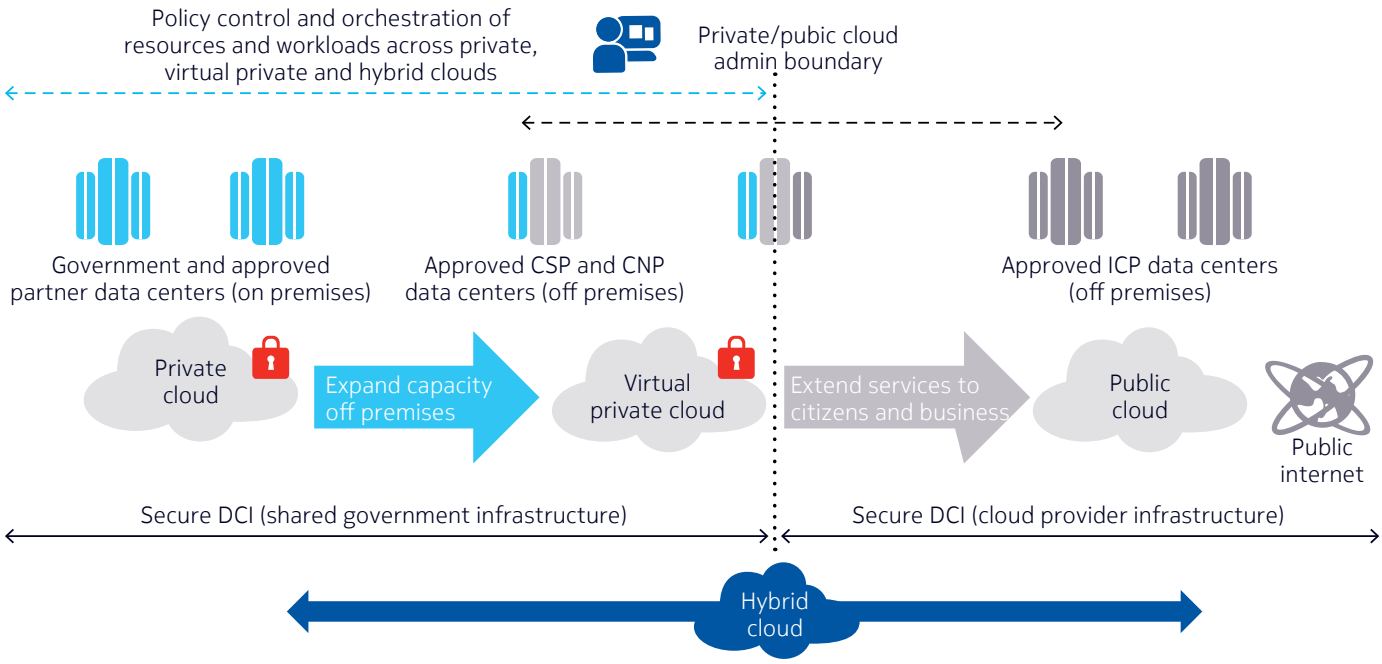
The ICP may host resources and services in its own data centers, or in CNP data centers and collocation facilities. Some cloud providers and SaaS providers locate their services in CNP facilities; others provide secure connectivity from them to their own facilities.

Public cloud services are best used for controlled access to non-critical applications and data because of potential data control, security, privacy and sovereignty concerns. Typically, government and the public sector use public cloud services to run non-critical applications and services where additional flexibility and elasticity are needed, or to host non-critical data and information for citizens or businesses.

Government hybrid clouds

A hybrid cloud model combines private and public cloud services and orchestrates resources across the private-public boundary, as shown in Figure 2. This approach requires strict policy control and the orchestration of resources across private, virtual private and hybrid clouds. It enables workloads and data to move between clouds based on factors such as the type of application, controlled access and consideration of data control, security and sovereignty. A hybrid cloud provides elasticity by enabling resources to expand and contract seamlessly to meet changing workloads.

Figure 2. Implementing a government hybrid cloud



The ultimate goal of the hybrid cloud is fluid, effortless workload portability across private and public cloud platforms. Hybrid cloud models offer greater agility and freedom because they combine the benefits of the private cloud with public cloud services. They offer the highest flexibility by enabling access to resources and services when, where and for as long as required. They also allow an organization to reduce CAPEX in favor of OPEX.

Nevertheless, the hybrid cloud model may not provide the level of control, security and compliance that many governments and public sector agencies mandate for some applications and data. Also, there are both business and technical challenges when implementing a hybrid cloud, particularly relating to the orchestration of network resources and service level agreements (SLAs) across the private-public cloud administrative boundary to achieve true service elasticity while maintaining performance and quality of service (QoS).

For these reasons, uptake of hybrid clouds by government and the public sector has been limited and slower than anticipated. Many governments have chosen to implement a form of hybrid cloud, in which private and virtual private clouds are used for critical applications and services, and are augmented by public cloud services for non-critical applications and services. This approach ensures that the necessary control, security and compliance measures can be implemented to run critical applications and store and process restricted or personal data. It also does not compromise on national security from inside and outside threats. While it delivers many benefits of the cloud, this approach stops short of allowing applications and data to move freely between clouds with seamless expansion and contraction of resources and workloads.

Government cloud initiatives

Many governments have established cloud initiatives to promote government-wide adoption of the cloud. These government cloud initiatives focus on the ability of the cloud to contribute to economic growth, capitalize on the cloud's promise of cost savings and create a more efficient, flexible and agile way of delivering public services. Government cloud has a number of attractions:

- **IT consolidation:** Consolidating multiple data centers into fewer larger facilities with common architecture built on open standards allows government departments and public sector agencies to reduce costs and increase operational efficiency. Fewer data center facilities reduce real-estate costs, lower energy consumption and improve green footprint significantly. Using commodity servers and implementing server virtualization reduce IT costs and improve resource utilization and efficiency. IT consolidation encourages migration from costly legacy systems, reduces overall operating costs significantly and ensures that applications and services are more consistent, and that data is more centralized and secure.

- **Shared services:** Governments and public sector agencies want to share IT to reduce costs and improve business process efficiency. Cloud adoption allows applications and services to be integrated and shared across multiple government departments and public sector agencies. Common data access and security procedures make data sharing and collaboration among agencies and departments much simpler.
- **Citizen services:** Almost all governments and public sector agencies provide a level of online services with self-service capabilities; for example, enabling citizens to access information online, request new services, amend existing ones, or enhance citizens' awareness of local, state or federal initiatives. Open government initiatives and online services also serve to inform and empower citizens.

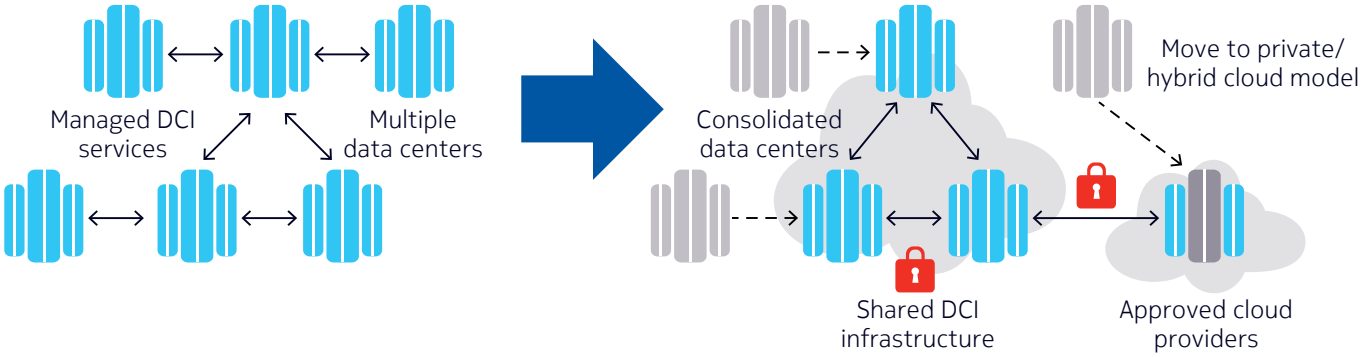
To address control, security and compliance concerns, many governments have created frameworks for the implementation of the government cloud. Many have implemented a form of hybrid cloud in which private clouds are augmented by approved cloud solutions that deliver generic ICT services as part of a secure online market place. The online market place may include IaaS, PaaS, SaaS and consulting services from approved vendors. Government departments and public sector agencies typically purchase approved cloud applications and services on a pay-as-you-go or yearly contract basis from the market place.

Typically, the government contracts with one or more cloud service providers, and government-approved cloud applications and services run on their cloud platforms. Often this includes applications and services from large cloud vendors as well as open source projects. A cloud authority oversees the government cloud to enforce standards and certification for commodity services. This authority also provides support for government departments, agencies and the public sector and resolves any cross-organizational issues.

Using approved cloud service providers offers substantial cost savings and increased flexibility. However, as discussed previously, data security, privacy and sovereignty restrictions prevent some services from being hosted or provided through public cloud services. In such cases, private and virtual private clouds are used to run critical applications, with public cloud services used to run non-critical applications or where additional flexibility and elasticity are required.

Governments and public sector agencies can reuse existing infrastructure and assets to implement their own private and virtual private clouds. They can also supplement these with approved third-party solutions to create their own hybrid cloud models. Typically, this involves consolidating government-owned data centers, and creating shared network infrastructure for DCI, as shown in Figure 3.

Figure 3. Consolidated data centers and shared DCI infrastructure



1. Consolidate and transform multiple data centers to reduce costs and increase efficiency
2. Implement shared DCI infrastructure for capacity, control and security
3. Enable data center virtualization and evolution to agile and flexible private/hybrid cloud models

Consolidating data centers and creating shared DCI infrastructure

Consolidating multiple data centers into fewer larger facilities with common architecture built on open standards allows common applications and services to be integrated and shared. Common data access and security procedures makes the sharing of data and collaboration among departments and agencies much simpler to implement and control. This can significantly reduce operating costs while ensuring that data and services are more consistent, centralized and secure.

As an example, data center consolidation and shared DCI infrastructure are at the center of the IT reforms by the Office of Management and Budget (OMB) in the US as part of its drive to cut down on duplicated spending by federal agencies. According to a report published by the U.S. Government Accountability Office (GAO)[1], the OMB's work has resulted in $US3.6 billion in cost savings from 2011 to 2014, of which $2 billion of savings have been attributed to data center consolidation and optimization projects across 24 participating federal agencies.

Another example is the Dutch government's project to consolidate its data centers, an important part of its cloud initiative. During 2013 and 2014, this project consolidated 66 separate data centers into four new and modern data centers forming the foundation for a private government cloud.[2] The data centers are interconnected securely using private shared DCI infrastructure that also provides secure connectivity to local government

1 Billions of dollars in savings have been realized, but agencies need to complete reinvestment plans, GAO-15-617, September 15, 2015

2 Cloud for Europe, FP7-610650, December 2014

and public sector agencies. As the existing networks have national coverage, this shared infrastructure provides secure connectivity without any dependency on the internet.

Consolidated data centers and creating shared DCI infrastructure provide the foundation for the Dutch government's iStrategy, which aims to transform government services to make them more easily available to citizens and businesses.[3] The goals of the project are to unify the fragmented ICT infrastructure, establish a single central government ICT security authority, and harmonize the services provided by central government to the public. Digital services in the Netherlands are a popular way of interacting with the government. According to a Deloitte report from November 2014, 79 percent of the population used e-government services in the previous year compared to an EU average of 41 percent.

Addressing shared DCI infrastructure concerns

Government and public sector projects can be particularly volatile. Decision makers are often only in position for a few years, and direction and priorities can change frequently. This creates uncertainty over budgets and a lack of commitment to projects that can be counterproductive to IT transformation.

Projects to consolidate data centers and create shared DCI infrastructure are more likely to be supported if they are understood to be essential to and part of government cloud strategy. In many cases, they are rightly considered to be strategic investments to enable the government cloud, particularly if they demonstrate business benefits in addition to the benefits of the cloud; for example, additional cost savings, greater resource efficiency, better collaboration and improved governance.

Consolidating data centers and creating a shared DCI infrastructure also involve technical challenges. For example, the cloud, the services it offers, the data centers that host these services and the DCI infrastructure that supports them must be available at all times—without fail and particularly at times of crisis. Fortunately, the cloud is inherently resilient. For example, server virtualization across data centers and mirrored services between different cloud types, for example between a private cloud and a virtual private cloud, create a high level of service resiliency.

However, ensuring that critical government cloud services remain available at all times requires additional measures that, when combined, can contribute significantly to cloud service resiliency and availability:

- Well-thought-out data center backup and recovery procedures to provide a robust BCDR solution

3 The Netherlands' iStrategy, Policy Note, 31 March 2012

- Redundant network connectivity, data switching and path protection to support high service availability in event of network or equipment failures
- Carrier-grade network technology and equipment to ensure five nines network availability and reliability as well as network control, security and integrity
- Agile and flexible network provisioning, management and troubleshooting across multiple layers to enable agile and flexible service management
- Security, encryption and intrusion detection implemented at multiple levels to protect against cyber-attack and ensure data privacy and integrity.

Data security and citizen privacy are paramount for government and public sector agencies. This means encrypting data using strong encryption and key exchange algorithms, both when at rest and in flight across the network. The system that generates and manages the encryption keys and ciphers must be separate from the network management system so that security and network operations can be carried out by completely separate operational groups. Where necessary, mechanisms should be deployed in the network to detect tampering and physical intrusion, with automatic network alerts triggered when a breach is detected.

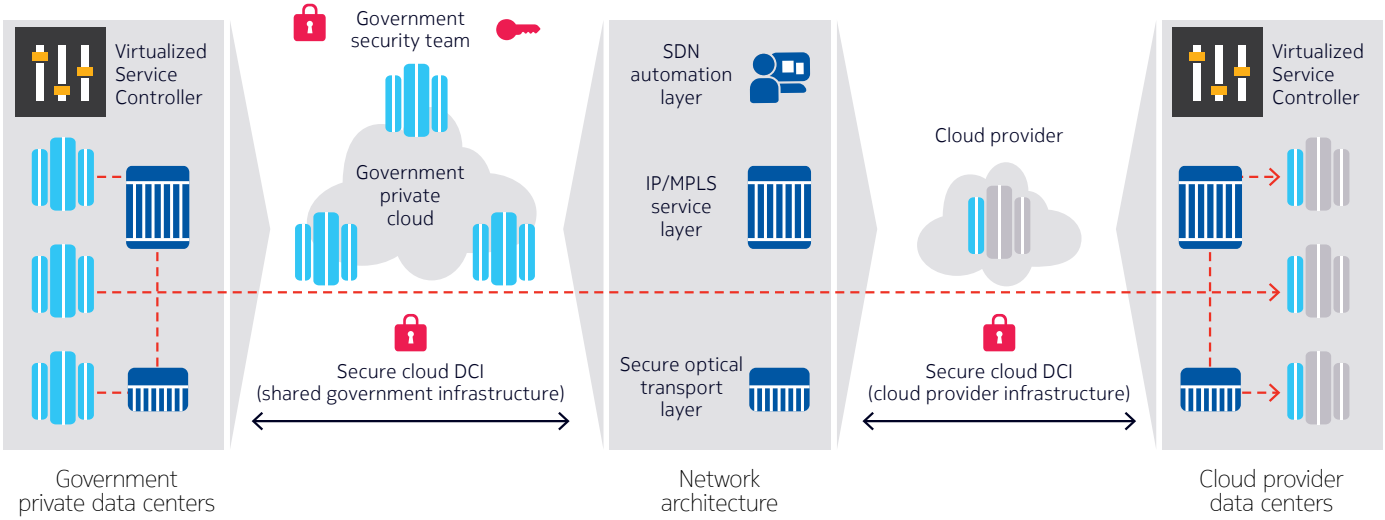
Cloud DCI—shared network infrastructure for the government cloud

Shared DCI infrastructure for the government cloud needs to ensure sustainable, reliable, anytime connectivity for citizens, government departments and public sector agencies alike. Such DCI infrastructure needs to:

- Enable the evolution to a distributed cloud-based architecture with minimal network impact
- Support flexible cloud deployment models; for example deliver services in the private cloud and provide access to approved public cloud services
- Provide a resilient and cost-effective WAN architecture for shared cloud services and robust BCDR
- Offer greater flexibility in network design and lower the barrier for new service introduction
- Simplify network management and service orchestration and offer more agile and dynamic service provisioning
- Allow the future automation of network operations while maintaining the high performance of virtualized applications
- Create an ROI model that quantifies the operational benefits of shared infrastructure.

These requirements are best served by cloud DCI, as shown in Figure 4. This approach provides a scalable, secure optical transport network that provides capacity and flexibility with an IP/MPLS services layer, which provides separation and control of inter- and intra-data center traffic.

Figure 4. Cloud DCI for secure, seamless interworking between cloud data centers



Cloud DCI also includes an SDN overlay that can be used to extend server virtualization and SDN between multiple data centers, simplifying virtual machine mobility between data centers and enabling seamless integration of data centers with existing network services and remote sites. Integrated network management complemented by SDN enables automation and optimization of cloud services to ensure lower operating costs and greater network control and efficiency.

Cloud DCI offers several advantages over traditional DCI solutions, including:

- **Scalable, flexible bandwidth:** The cloud creates a demand for very high and easily scalable bandwidth. Cloud DCI supports very high bandwidth and optical wavelength, Ethernet and IP capabilities for different cloud applications—and allows bandwidth to be increased and decreased flexibly as needed.
- **Multi-site, multi-technology, multi-cloud capabilities:** Cloud DCI helps to share data, distribute applications and balance workloads more easily across different cloud types, between multiple locations and between different cloud providers. It provides multi-site, multi-technology capabilities with the high performance, reliability and QoS required to connect multiple data centers in the cloud.
- **Agile, dynamic provisioning:** Cloud DCI supports orchestration of network resources across cloud boundaries to ramp up or turn down resources when and where required. It supports provisioning of bandwidth and orchestrates network resources dynamically, quickly and easily—between different locations, across multiple data centers and across different types of cloud.

Cloud DCI delivers the capacity, flexibility and security government and the public sector need for fast turn-up of cloud services. At the same time, cloud DCI helps ensure business continuity, improve asset utilization and reduce costs.

The benefits of cloud DCI

Implementing cloud DCI has several key benefits, including:

- **Security:** Cloud DCI offers more secure transport connections than the public internet. When cloud DCI is combined with existing shared infrastructure and managed services (such as IP VPNs), multiple large sites, branch offices and remote locations can also use cloud resources securely.
- **Cost:** Cloud DCI can reduce costs because traffic is not routed over a CPS's internet or IP VPN service. Instead, traffic is transported directly to the cloud over dark fiber. Cloud DCI can also use managed wavelengths or Carrier Ethernet, which generally offers much higher bandwidth at less cost than an IP VPN service.
- **Performance:** Bandwidth, latency, response time, QoS and reliability are more consistent with private cloud DCI. Depending on the technology used, the link can support latency-sensitive applications and workloads that cannot run over the public internet.
- **Flexibility:** Access to a variety of cloud services, including virtual private, hybrid and public, can be implemented over the same cloud DCI link. As a result, different workloads can be allocated to resources that have the appropriate price/performance profile.

Nokia cloud DCI solutions

Nokia offers a choice of cloud DCI solutions that provide the scalability, security and control to support current government and public sector DCI needs—along with the agility, flexibility and performance needed to support cloud interconnect across different cloud types. Nokia cloud DCI solutions provide a multi-layer architecture that includes carrier-grade optical transport, IP/MPLS routing and SDN solutions for both the data center and the WAN. With combined IP/optical management and automated and on-demand networking using SDN, Nokia can deliver agile, dynamic, flexible and cost-effective cloud DCI solutions.

Nokia DCI solutions are used by many governments and public sector agencies as well as large enterprises in the financial, healthcare, consumer and industrial sectors for business-critical DCI applications such as BCDR. They are widely deployed in the oil and gas, transportation and utility sectors for mission-critical DCI applications, and are used by many service providers and network operators worldwide.

To find out more, please visit the Nokia Cloud Data Center Interconnect solution page or see the Cloud DCI solutions for enterprise and public sector application note.

NOKIA

Acronyms

BCDR	business continuity and disaster recovery
CAPEX	capital expenditures
CNP	carrier-neutral provider
CSP	communications service provider
DCI	data center interconnect
IaaS	infrastructure as a service
ICP	internet cloud (or content) provider
ICT	information communications infrastructure
MPLS	Multiprotocol Label Switching
MTDC	multi-tenant data center
OPEX	operating expenditures
PaaS	platform as a service
QoS	quality of service
ROI	return on investment
SaaS	software as a service (SaaS)
SDN	software-defined networking
SLA	service level agreement
VPN	virtual private network

Nokia Oyj
Karaportti 3
FI-02610 Espoo
Finland
Tel. +358 (0) 10 44 88 000

Product code: SR10001146EN (November)